UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

69151 7590 02/17/2010

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
02/17/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GREGORY NEIL HOUSTON, CHRISTIAN D. KOBSA,
SRIDHAR EMBAR, MATTHEW THADDEUS DIIORIO,
BRYAN DOUGLAS WILLIAMS, and MICHAEL GEORGE NIKITAIDES

Appeal 2008-005057
Application 09/844,448
Technology Center 2100

Decided: February 17, 2010

Before LEE E. BARRETT, JOHN A. JEFFERY, and
DEBRA K. STEPHENS, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-59. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

This invention relates to a method for managing security event data collected from a computing network. Event managing software collects and processes security event data from security devices. A user can create customized "scopes" of varying criteria to analyze and filter the data. The data can be used to respond to a security event. *See generally* Abstract; Spec. 2-3; Figs. 1-2. Claim 27 is illustrative:

> 27. A computer-implemented system for managing security event data collected from a plurality of security devices comprising:
>
> a plurality of security devices operable for generating security event data comprising a plurality of alerts that are generated in response to detecting a security event in a distributed computing environment;
>
> an event manager coupled to the security devices, the event manager operable for collecting the security event data from the security devices and analyzing and filtering the security event data with scope criteria comprising one or more definable variable operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security even, a security event type, a priority of a security event, and an identification of a system that detected a security event, and applying the scope criteria to the security event data to produce result data; and
>
> one or more clients coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager and displaying the result data comprising filter alerts based on the scope criteria.

The Examiner relies on the following as evidence of unpatentability:

Hill	US 6,088,804	July 11, 2000
Baker	US 6,775,657 B1	Aug. 10, 2004

THE REJECTIONS

1. The Examiner rejected claims 27-29, 31, and 32 under 35 U.S.C. § 102(e) as anticipated by Hill. Ans. 3-6.[1]
2. The Examiner rejected claims 1-26, 30,[2] and 33-59 under 35 U.S.C. § 103(a) as unpatentable over Hill and Baker. Ans. 6-13.

CLAIM GROUPING

Appellants argue independent claim 27 (Br. 13-17) in connection with the anticipation rejection, but do not separately argue dependent claims 28, 29, 31, and 32 with particularity despite grouping them under a separate heading.[3] *See* Br. 17. Accordingly, we group claims 27-29, 31, and 32 together and select claim 27 as representative of that group. *See* 37 C.F.R. § 41.37(c)(1)(vii).

THE ANTICIPATION REJECTION

Regarding representative claim 27, the Examiner finds that Hill discloses a computer security management system with every claimed feature including an "event manager" (self-organizing map (SOM) processor

---

[1] We refer to the Appeal Brief filed February 20, 2007 and the Examiner's Answer mailed June 28, 2007 throughout this opinion.

[2] Although the Examiner omits claim 30 in the statement of this rejection in the Answer, the Examiner nonetheless includes claim 30 in the corresponding rejection in the Final Rejection mailed November 17, 2006. *Compare* Ans. 6 *with* Final Rej. 7, 10. Accordingly, we presume that the Examiner intended to include claim 30 in this rejection.

[3] Although Appellants indicate that claim 33 depends from claim 27 in connection with this grouping (Br. 17), claim 33 actually depends from claim 1. We therefore treat this claim in connection with the Examiner's obviousness rejection along with other dependent claims so rejected.

40) that is said to collect security event data from various "security devices" connected on a network. According to the Examiner, Hill's SOM processor analyzes and filters this collected data with "scope criteria," namely using Hill's attack signatures to determine and display the type, location, and severity of the security event. Ans. 3-5.

Appellants argue that Hill merely displays attack status information, but does not analyze and filter security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the data as claimed. Br. 13-17.

The issue before us, then, is as follows:

ISSUE

Under § 102, have Appellants shown that the Examiner erred in rejecting claim 27 by finding that Hill analyzes and filters security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the data?

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence:

Hill

1. Hill discloses a dynamic network security system 20 for adaptively responding to computer network security attacks. The system includes multiple security agents 36 that detect occurrences of

"security events" (e.g., port scans, malicious software, penetration attempts, etc.) on associated computer nodes 24. This collected security event data is transmitted to a self-organizing map (SOM) processor 40 which processes the data using artificial neural network technology. Hill, col. 1, ll. 6-9; col. 4, ll. 5-61; Fig. 1.

2. SOM processor 40 processes security events to form an attack signature. Network status display 42 displays attack status information in accordance with the attack signature. Hill, col. 5, ll. 7-20; Fig. 1.

3. The system is first trained by accessing a database 48 of simulated attack information. As shown in Figure 3, this database includes different operator-generated simulated attacks 52 which predict a particular type of attack. Hill, col. 5, ll. 22-45; Figs. 2-3.

3A. Simulated attacks 52 are generated by an operator and stored in database 48. These predictions can be developed using network modeling tools or static analyzers and are based on historical data, attack trends, perceived threats, etc. Hill, col. 5, ll. 41-45.

4. Training signatures 53 for simulated attacks 52 are defined by plural security events of at least one security event type 56 (e.g., destructive virus, worm, Trojan horse, FTP requests, and network overload). Hill, col. 5, ll. 46-65; Fig. 3.

5. Training signatures also include location identifiers 60 that identify the nodes 24 in the network where security events occur. Location identifiers are important for ascertaining an attack severity 61 for each simulated attack. Hill, col. 5, l. 66 – col. 6, l. 22; Figs. 1-3.

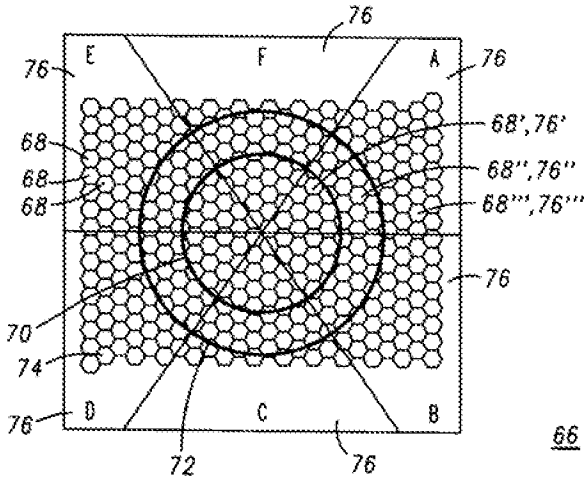
6. A first simulated attack 55 is then input into the system, and the SOM processor maps the first training signature into the network status display 42. Hill, col. 6, ll. 24-35; Fig. 2.

7. The network status display includes a display map 66 that is divided into multiple display cells 68. The SOM processor plots a vector representative of the first training signature onto the array of display cells. The map also includes three regions that represent different attack severity levels as follows:

Region	Severity
Center (70)	Low
Middle (72)	Medium
Outer (74)	High

Hill, col. 6, ll. 53-60; Fig. 4.

8. The display map's regions 70, 72, and 74 are further divided into subregions 76 which indicate an attack type (i.e., "A"-"F"). A "snooping virus" attack, for example, can be labelled as an attack type "A." Hill, col. 6, l. 61 – col. 7, l. 8. Hill's display map is shown in Figure 4 reproduced below:



Hill's Display Map of Figure 4

9. Following training, Hill's system can respond to actual attacks as outlined in Figure 5. In an actual attack situation, the SOM processor receives (1) data from security agents 36 including a security event type and location identifier, and (2) an attack signature. The SOM processor then compares a vector representative of the first attack signature 94 to each training signature 53 mapped in display map 66. The training signature that most closely matches the attack signature is then selected. Hill, col. 8, ll. 4-49; Figs. 4-6.

10. Figure 7 shows network status display 42 which includes (1) a display map 66; (2) an attack status information list 108 showing security event type 56 and location identifiers for the first attack 92; (3) an attack signature log 110; and (4) an attack mitigation list 112 which lists various possible mitigation actions. Hill, col. 8, l. 62 – col. 9, l. 7; Fig. 7. Hill's network status display is shown in Figure 7 reproduced below:

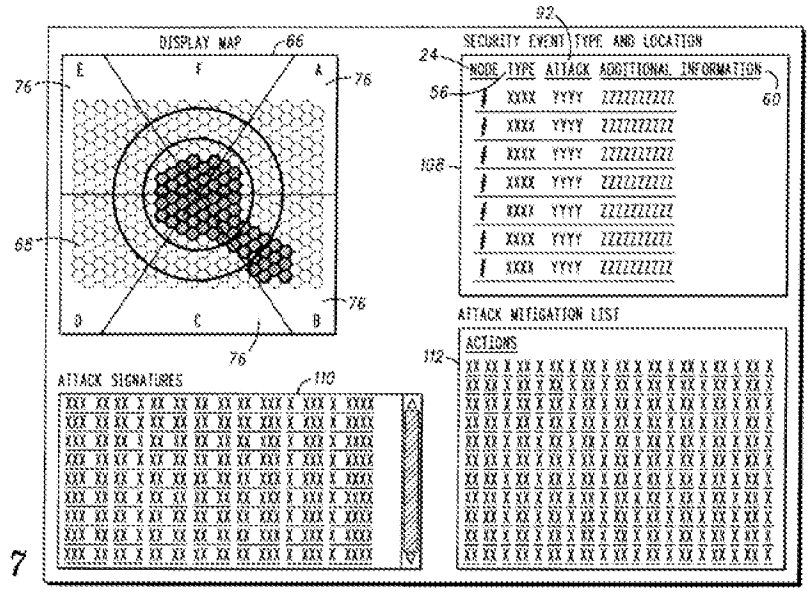


FIG. 7

Hill's Network Status Display in Figure 7

11. The attack status information list 108 in Hill's Figure 7 includes a legend indicating "SECURITY EVENT TYPE AND LOCATION," and labels columns of information as follows: "NODE," "TYPE," "ATTACK," and "ADDITIONAL INFORMATION." Information is provided in rows underneath the columns. Hill, Fig. 7.

12. By darkening various display cells 68, the display map 66 of Figure 7 graphically indicates the progression of an attack's severity over time (i.e., from a low severity attack in center region 70 to a high severity attack in outer region 74). Hill, col. 9, ll. 8-19; Fig. 7.

PRINCIPLES OF LAW

Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations. *RCA Corp. v. Appl. Dig. Data Sys., Inc.*, 730 F.2d 1440, 1444 (Fed. Cir. 1984); *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554 (Fed. Cir. 1983).

ANALYSIS

We see no error in the Examiner's reliance on Hill for disclosing an event manager that *analyzes and filters* security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the data as claimed.

We emphasize the terms "analyzes" and "filters" since the system of Hill must be operable to perform both of these functions to meet the claim. And we find—as does the Examiner (Ans. 15-16)—that Hill's SOM processor (i.e., the "event manager") analyzes and filters collected network event data to display information pertaining to a particular attack, namely the type, location, and severity of a particular security event. *See* FF 1, 2, 10-12. The Examiner's point in this regard (Ans. 15-16) is well taken.

Indeed, the very act of collecting information pertaining to network security events from the security agents 36 and comparing a received signature to the closest training signature for selection (FF 9) involves analyzing the security event data with "scope criteria." We reach this conclusion emphasizing that signatures for particular attacks are associated with a particular type of event, location, and severity. *See* FF 3-5.

The event manager likewise filters the collected security event data as evidenced by the display in Figure 7. As shown in that figure, the display map 66 graphically indicates the progression of an attack's severity over time by denoting samples regarding a particular attack via darkened display cells. FF 12. This change in severity level is readily apparent since the level of severity is indicated by darkened cells' placement within the map's center, middle, and outer regions. *See* FF 7, 12. Similarly, Hill's map also graphically indicates the type of attack depending on the subregion ("A"-"F") that a particular darkened display cell appears. *See* FF 8, 10.

Figure 7, for example, illustrates a severe "Type B" attack since its darkened cells are in the sub-region corresponding to that type of attack (i.e., the lower right sub-region labelled "B"). *See* FF 8, 10. This attack also has a high severity level since it is in the outer region. *See* FF 7, 10.

Graphically representing this information based on collected security event data would not only involve analyzing the collected information, but also filtering it to comport to the constraints of this graphical representation based on attack type and severity. *See* FF 7, 8, 10, 12. Moreover, Hill's information based on collected security event data in the status information list 108 of Figure 7 likewise would involve analyzing and filtering the collected security event data to comport to the particular tabular presentation of information based on event type and location. *See* FF 10-11.

Notably, these two criteria (type and location) are identical to two of the recited variables of the scope criteria in claim 27. Moreover, these criteria reasonably correspond to definable variables as claimed since these criteria are based on simulated attack information that is generated by an operator and stored in a database. FF 3-3A.

We are therefore not persuaded that the Examiner erred in rejecting representative claim 27, and claims 28, 29, 31, and 32 which fall with claim 27.

THE OBVIOUSNESS REJECTION

We will also sustain the Examiner's obviousness rejection of claims 1-26, 30, and 33-59 over Hill and Baker (Ans. 6-13). Appellants essentially reiterate similar arguments made in connection with claim 27. *See* Br. 17-21. Nor do Appellants particularly point out errors in the Examiner's reliance on Baker or dispute the references' combinability as the Examiner indicates (Ans. 18). We are therefore not persuaded that the Examiner erred in rejecting claims 1-26, 30, and 33-59 for the reasons previously discussed. The rejection is therefore sustained.

CONCLUSION

Appellants have not shown that the Examiner erred in rejecting (1) claims 27-29, 31, and 32 under § 102, and (2) claims 1-26, 30, and 33-59 under § 103.

ORDER

The Examiner's decision rejecting claims 1-59 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521